AGRÉGATION DES SCIENCES MATHÉMATIQUES

Composition de mathématiques générales. 1977

PREMIÈRE PARTIE

6165. Soit K un corps commutatif de caractéristique différente de 2. On appelle *espace quadratique* tout couple (E, Q), où E est un espace vectoriel de dimension finie sur le corps K et Q une forme quadratique non dégénérée sur E. On notera P la forme polaire de Q. Par abus de langage, on écrira souvent E pour (E, Q).

I. – 1° Soit (E, Q) et (E′, Q′) deux espaces quadratiques. On pose $E'' = E \times E'$ et on désigne par Q″ l'application

$$Q'' : E'' \to K \quad (x, x') \longmapsto Q(x) + Q'(x')$$

(relation abrégée en $Q'' = Q + Q'$). Montrer que le couple (E″, Q″) est un espace quadratique que l'on appellera *somme directe* de E et E′.

I. – 2° Soit π la projection canonique de E″ sur E, A un sous-espace de E″. A toute partie X de E, on associe $\overline{X} = X \times \{0\}$. On munit $\overline{E}$ de la forme quadratique $\overline{Q}$, telle que $\overline{Q}(x, 0) = Q(x)$. On note par les signes $\perp$, $\circ$ et $\bullet$ les orthogonalités dans les espaces E″, E et $\overline{E}$. Calculer $\overline{X}^{\perp}$ en fonction de X^0. Comparer $\pi(A^{\perp})$ et $\pi[(A \cap \overline{E})^{\bullet}]$. Déterminer l'orthogonal dans E″ du produit d'un sous-espace de E par un sous-espace de E′.

I. – 3° Définir à l'aide de Q une notion naturelle d'*isomorphisme quadratique* entre deux espaces quadratiques de façon que toute décomposition de E en somme directe de sous-espaces orthogonaux rende E isomorphe à la somme directe (au sens du 1°) de ces sous-espaces munis de formes convenables.

I. – 4° (E, Q) étant un espace quadratique, on note (abusivement) E^- le couple (E, − Q). Déterminer un sous-espace L de $E \times E^-$ égal à son orthogonal $L^{\perp}$.

I. – 5° Un espace quadratique est dit *hyperbolique* si, et seulement si, il admet un *lagrangien*, c'est-à-dire un sous-espace égal à son orthogonal.

Soient (E, Q) un espace quadratique hyperbolique et L un lagrangien de cet espace. Que peut-on dire de la dimension de E ?

On considère un supplémentaire L_0 de L, une base $(e_1, \ldots, e_n)$ de L et une base $(f_1, \ldots, f_n)$ de L_0. A tout vecteur $v \in E$ on associe les matrices-colonnes X et Y dont les éléments sont respectivement les n premières et les n dernières coordonnées de v dans la base $(e_1, \ldots, f_n)$ de E. Montrer qu'il existe deux matrices carrées d'ordre n, A et B, telles que, pour tout $v \in E$

$$Q(v) = {}^tXAY + {}^tYBY.$$

Montrer que la matrice A est inversible.

I. – 6° Montrer que l'on peut choisir L_0 et les bases $(e_1, \ldots, e_n)$, $(f_1, \ldots, f_n)$ de façon que, pour tout $v \in E$, $Q(v) = {}^tXY$. En déduire que, L^* désignant le dual de L, (E, Q) est quadratiquement isomorphe à (H(L), R), où H(L) désigne $L \times L^*$ et où R est déterminé par

$$R(x, \varphi) = \varphi(x).$$

I. – 7° On remplace maintenant l'hypothèse $L^\perp = L$ par l'inclusion $L \subset L^\perp$. Soit Λ un supplémentaire de L dans $L^\perp$. Déduire de la question précédente que l'on peut munir l'espace quotient $L^\perp/L$ d'une forme quadratique telle que E soit quadratiquement isomorphe à la somme directe $(L^\perp/L) \times H(L)$, (H(L) est défini comme au 6°; on pourra rechercher un lagrangien de $\Lambda^\perp$).

I. – 8° Soit E et E' deux espaces quadratiques tels que les espaces E' et $E \times E'$ admettent des lagrangiens notés respectivement U et T. Posant $\overline{\overline{U}} = \{0\} \times U$, montrer (avec les notations du 2°) que $\pi[(T + \overline{\overline{U}}) \cap \overline{E}]$ est un lagrangien de E.

I. – 9° On dira que deux espaces quadratiques E et E' sont *équivalents* si $E \times (E')^-$ est hyperbolique. Justifier l'emploi de l'adjectif « équivalent ». Admettant que les classes d'équivalence définies par cette relation forment un ensemble, munir cet ensemble d'une addition de façon à obtenir un groupe abélien qui sera noté W(K).

Montrer que W(**C**) et W(**R**) sont respectivement isomorphes aux groupes $\mathbf{Z}/2\mathbf{Z}$ et **Z**.

DEUXIÈME PARTIE

II. – 1° Soit $\mathbf{F}_q$ un corps fini commutatif de cardinal q et de caractéristique différente de 2, et (a, b) un couple d'éléments non nuls de $\mathbf{F}_q$. Dénombrer les éléments de $\mathbf{F}_q$ de la forme $1 - by^2$ et montrer que l'équation $ax^2 + by^2 = 1$ a au moins une solution $(x, y) \in \mathbf{F}_q^2$.

II. – 2° Soit (E, Q) un espace quadratique sur $\mathbf{F}_q$. Montrer l'existence d'une base $(e_1, \ldots, e_n)$ de E orthogonale relativement à Q, telle que, pour $i \geqslant 2$, $Q(e_i)$ soit égal à 1. Montrer que, pour que l'on puisse imposer la condition supplémentaire $Q(e_1) = 1$, il faut, et il suffit, que le déterminant de Q relatif à une base quelconque soit un carré dans $\mathbf{F}_q$.

II. – 3° En écrivant l'identité polynomiale

$$X^{q-1} - 1 = (X^r - 1)(X^r + 1), \quad \text{où} \quad r = \frac{q-1}{2},$$

montrer que, pour tout $a \in \mathbf{F}_q$, la condition $a^r = 1$ équivaut à l'existence d'un élément non nul $b \in \mathbf{F}_q$ tel que $a = b^2$. On examinera les cas

$$q = 4m + 1 \quad \text{et} \quad q = 4m + 3.$$

II. – 4° Montrer que, selon que $q = 4m + 1$ ou $q = 4m + 3$, $W(\mathbf{F}_q)$ est isomorphe à $(\mathbf{Z}/2\mathbf{Z})^2$ ou à $\mathbf{Z}/4\mathbf{Z}$ (on pourra introduire un élément $\omega \in \mathbf{F}_q$ qui n'est pas un carré et considérer $(\mathbf{F}_q, Q)$, où $Q(x)$ désigne x^2 ou ωx^2).

TROISIÈME PARTIE

III. – 1° Soit G un groupe abélien fini noté additivement. On sait qu'il existe k nombres premiers (distincts ou non) $p_1, \ldots, p_k$ et k entiers non nuls $n_1, \ldots, n_k$ tels que, si l'on pose $q_i = p_i^{n_i}$ $(1 \leqslant i \leqslant k)$, G soit isomorphe au produit direct

$$(\mathbf{Z}/q_1\mathbf{Z}) \times (\mathbf{Z}/q_2\mathbf{Z}) \times \ldots \times (\mathbf{Z}/q_k\mathbf{Z}),$$

la famille $(q_1, \ldots, q_k)$ étant unique à l'ordre près.

Soit $\widehat{G} = \mathrm{Hom}\,(G, \mathbf{Q}/\mathbf{Z})$ le groupe des homomorphismes de G dans le groupe-quotient du groupe additif de **Q** par le sous-groupe **Z**.

Montrer que G et $\widehat{G}$ ont même cardinal.

III.—2° Soit χ l'application de G dans $\widehat{\widehat{G}}$ définie par les relations :

$$\chi : G \to \widehat{\widehat{G}}, \qquad \chi(x) : \widehat{G} \to \mathbf{Q}/\mathbf{Z}, \qquad \chi(x)(\varphi) = \varphi(x).$$

Montrer que χ est un isomorphisme de groupes.

III.—3° Soit h une application de $G \times G$ dans $\mathbf{Q}/\mathbf{Z}$ supposée *symétrique* (c'est-à-dire telle que $h(x, y) = h(y, x)$ pour tout couple (x, y)) et en outre *bilinéaire* (c'est-à-dire telle que $h(x + x', y) = h(x, y) + h(x', y)$ pour tout triplet (x, x', y)). On note $\bar{h}$ l'homomorphisme défini par les relations

$$\bar{h} : G \to \widehat{G}, \qquad \bar{h}(x) : G \to \mathbf{Q}/\mathbf{Z}, \qquad \bar{h}(x)(y) = h(x, y).$$

Montrer que $\bar{h}$ est un isomorphisme si, et seulement si, h est *non dégénérée* (c'est-à-dire si, à tout $x \neq 0$, correspond au moins un y tel que $h(x, y) \neq 0$). On dira alors que (G, h) est un *groupe bilinéaire*. Par abus de langage, on écrira souvent G pour (G, h).

III.—4° On appliquera désormais aux groupes bilinéaires langage et notations des espaces quadratiques : on dira par exemple que les parties X et Y du groupe bilinéaire G sont orthogonales si, pour tout $(x, y) \in X \times Y$, $h(x, y) = 0$; on notera n le cardinal de G, et, pour tout nombre premier i, G_i le sous-groupe des $x \in G$ tels que $i^n x = 0$. Montrer qu'il existe un nombre premier p tel que G soit bilinéairement isomorphe au produit direct de sous-groupes $G_2 \times G_3 \times G_5 \times \ldots \times G_p$, chaque partie G_i $(i \leqslant p)$ étant orthogonale aux autres.

III.—5° L et L′ étant deux sous-groupes de G, on notera $L + L'$ le sous-groupe de G engendré par $L \cup L'$. Montrer que l'orthogonal de L est un sous-groupe $L^\perp$ de G. Montrer que tout homomorphisme $\lambda \in \widehat{L}$ peut être prolongé en un homomorphisme $\bar{\lambda} \in \widehat{G}$. Vérifier les égalités

$$\operatorname{card} L^\perp = \frac{\operatorname{card} G}{\operatorname{card} L}, \qquad L^{\perp\perp} = L, \qquad (L + L')^\perp = L^\perp \cap L'^\perp, \qquad L^\perp + L'^\perp = (L \cap L')^\perp.$$

III.—6° Si la restriction de h à L est non dégénérée, montrer que G est bilinéairement isomorphe au produit direct $L \times L^\perp$.

III.—7° On note encore (abusivement) G^- le couple $(G, -h)$. En supposant $L \subset L^\perp$, munir $L^\perp/L$ d'une forme bilinéaire, symétrique, non dégénérée, naturellement liée à h, telle que le groupe bilinéaire $(L^\perp/L) \times G^-$ qui s'en déduit admette un sous-groupe Γ égal à son orthogonal (on pourra considérer la surjection canonique τ de $L^\perp$ sur $L^\perp/L$ et l'ensemble des couples $(\tau(x), x)$ où $x \in L^\perp$).

III.—8° On dira que deux groupes bilinéaires G et G′ sont *équivalents* si $G \times (G')^-$ admet un sous-groupe égal à son orthogonal. Montrer, en s'inspirant du I, 9°, que l'on peut définir un groupe abélien $\mathscr{W}$ analogue aux différents W(K).

III.—9° Si p est un nombre premier, on appelle *groupe p-primaire* un groupe additif G tel que $G = G_p$ (avec la notation du III.—4°). Montrer que les classes d'équivalence des groupes bilinéaires p-primaires définissent un sous-groupe $\mathscr{W}_p$ de $\mathscr{W}$. Montrer que $\mathscr{W}$ est isomorphe au sous-groupe de $\mathscr{W}_2 \times \mathscr{W}_3 \times \mathscr{W}_5 \times \ldots \times \mathscr{W}_p \times \ldots$ constitué par les suites (x_i), (i premier; $x_i \in \mathscr{W}_i$), qui n'ont qu'un nombre fini de termes non nuls.

III.—10° Montrer que $\mathscr{W}_p$ est isomorphe à $\mathbf{Z}/2\mathbf{Z}$ si $p = 2$, et isomorphe à $W(\mathbf{F}_p)$ si $p \geqslant 3$ (on pourra montrer que si G est bilinéaire et s'il existe $m \geqslant 2$ tel que $p^m x = 0$ pour tout $x \in G$, alors il existe un groupe bilinéaire équivalent à G, et un entier $m' < m$ tel que $p^{m'} y = 0$ pour tout $x \in G'$).

QUATRIÈME PARTIE.

Un groupe additif abélien est dit *libre de type fini* s'il existe un entier n tel que le groupe soit isomorphe à $\mathbf{Z}^n$. Soit H un tel groupe. Nous admettrons que les sous-groupes de H sont également libres de type fini; nous noterons $H^* = \operatorname{Hom}(H, \mathbf{Z})$ le groupe des homomorphismes de H dans le groupe $\mathbf{Z}$.

IV.—1° Montrer que H et H* sont isomorphes.

IV.—2° Soit E et F deux groupes abéliens libres de type fini et $\alpha : E \to F$ un homomorphisme. On appelle *transposé* de α l'homomorphisme ${}^t\alpha : F^* \to E^*$ défini par ${}^t\alpha(\varphi) = \varphi \circ \alpha$, et *conoyau* de α le groupe-quotient

$G = \operatorname{Coker} \alpha = F/\alpha(E)$; on suppose que le conoyau de α est fini. Comme au III, on note $\widehat{G} = \operatorname{Hom}(G, \mathbf{Q}/\mathbf{Z})$.
Montrer que ${}^t\alpha$ est injectif.

IV. – 3° On considère en outre un élément $w \in \widehat{G}$. On désigne par $\beta : \mathbf{Z} \to \mathbf{Q}$, $\gamma : \mathbf{Q} \to \mathbf{Q}/\mathbf{Z}$, $\delta : F \to G$ les homomorphismes canoniques. Montrer qu'il existe des homomorphismes $v : F \to \mathbf{Q}$, $u : E \to \mathbf{Z}$ tels que le diagramme

$$\begin{array}{ccccc} E & \xrightarrow{\alpha} & F & \xrightarrow{\delta} & G \\ {\scriptstyle u}\downarrow & & {\scriptstyle v}\downarrow & & {\scriptstyle w}\downarrow \\ \mathbf{Z} & \xrightarrow{\beta} & \mathbf{Q} & \xrightarrow{\gamma} & \mathbf{Q}/\mathbf{Z} \end{array}$$

soit commutatif.

IV. – 4° Soit réciproquement $u \in E^*$. Supposant de plus α injectif, montrer qu'il existe v et w tels que le diagramme ci-dessus soit commutatif, et qu'ils sont uniques. Montrer que la correspondance définie par $u \longmapsto w$ induit un homomorphisme surjectif de E^* sur $\widehat{G}$, de noyau ${}^t\alpha(F^*)$, et que $\operatorname{Coker} {}^t\alpha$ est isomorphe à $\widehat{G}$.

IV. – 5° Soit $A = (a_{ij})$ une matrice symétrique à coefficients dans $\mathbf{Z}$, de déterminant $\det A \neq 0$; soient $\alpha : \mathbf{Z}^n \to \mathbf{Z}^n$ et $\alpha' : \mathbf{Q}^n \to \mathbf{Q}^n$ les homomorphismes représentés par A dans les bases canoniques respectives. Pour tout couple $(a, b) \in (\mathbf{Q}^n)^2$, où $a = (a_1, \ldots, a_n)$, $b = (b_1, \ldots, b_n)$, on pose $a \bullet b = \sum_{i=1}^{n} a_i b_i$. Si δ est l'homomorphisme canonique de $\mathbf{Z}_n$ sur $G = \operatorname{Coker} \alpha = \mathbf{Z}^n/\alpha(\mathbf{Z}^n)$, on définit une application bilinéaire symétrique h de $G \times G$ dans $\mathbf{Q}/\mathbf{Z}$ par l'égalité

$$h(\delta(x), \quad \delta(y)) = \gamma(\alpha'^{-1}(x) \bullet y).$$

Montrer que (G, h) est un groupe bilinéaire.

IV. – 6° Soit L un sous-groupe de G. Montrer que $\Phi = \delta^{-1}(L)$ contient $\alpha(\mathbf{Z}^n)$ et que, si $j : \Phi \to \mathbf{Z}^n$, $k : L \to G$ sont les homomorphismes canoniques, il existe des homomorphismes $s : \mathbf{Z}^n \to \Phi$, $\varepsilon : \Phi \to L$ tels que le diagramme

$$\begin{array}{ccccc} \mathbf{Z}^n & \xrightarrow{\alpha} & \mathbf{Z}^n & \xrightarrow{\delta} & G \\ & {\scriptstyle s}\searrow & {\scriptstyle j}\uparrow & & \uparrow{\scriptstyle k} \\ & & \Phi & \xrightarrow{\varepsilon} & L \end{array}$$

soit commutatif.

IV. – 7° On suppose que $L \subset L^\perp$ et on note $\rho : \Phi \to \Phi^*$ l'homomorphisme défini par $\rho(x)(y) = \alpha'^{-1}(x) \bullet y$; montrer que, si e est l'isomorphisme de $\mathbf{Z}^n$ sur $(\mathbf{Z}^n)^*$ déduit de la forme bilinéaire $(a, b) \longmapsto a \bullet b$, le transposé de s est tel que

$${}^t s \circ \rho = e \circ j.$$

IV. – 8° On suppose $L = L^\perp$; montrer que ρ est un isomorphisme. Si $(f_1, \ldots, f_n)$ engendre Φ et si B est la matrice de la forme bilinéaire $(x, y) \longmapsto \alpha'^{-1}(x) \bullet y$ dans cette base de Φ, montrer que $|\det B| = 1$.

IV. – 9° Montrer que, si $n = 2$, $A = 2I$, L étant engendré par la classe modulo $\alpha(\mathbf{Z}^2)$ du vecteur $(1, 1)$, on se trouve dans la situation du IV.-8°, et déterminer alors Φ, ρ, s et ε.

IV. – 10° On suppose que $p_1, \ldots, p_q$ sont q nombres premiers deux à deux distincts, de la forme $(4k + 1)$, et que

$$\det A = 2^{r_0} p_1^{r_1} \ldots p_q^{r_q}.$$

Montrer qu'il existe des matrices S et C à coefficients dans $\mathbf{Z}$ et d'ordre $2n$ telles que l'on ait les égalités

$$\det C = 1, \qquad {}^t\mathrm{SCS} = \begin{bmatrix} A & 0 \\ 0 & A \end{bmatrix}.$$